

Attachment 1

U.S. Commercial Nuclear Power Plants That Are Licensed to Operate

Power plant	City	State	NRC region
Arkansas Nuclear 1	Russellville	AR	4
Arkansas Nuclear 2	Russellville	AR	4
Beaver Valley 1	McCandless	PA	1
Beaver Valley 2	McCandless	PA	1
Braidwood 1	Joilet	IL	3
Braidwood 2	Joilet	IL	3
Browns Ferry 1	Decatur	AL	2
Browns Ferry 2	Decatur	AL	2
Browns Ferry 3	Decatur	AL	2
Brunswick 1	Southport	NC	2
Brunswick 2	Southport	NC	2
Bryon 1	Rockford	IL	3
Bryon 2	Rockford	IL	3
Callaway	Fulton	MO	4
Calvert Cliffs 1	Annapolis	MD	1
Calvert Cliffs 2	Annapolis	MD	1
Catawba 1	Rock Hill	SC	2
Catawba 2	Rock Hill	SC	2
Clinton	Clinton	IL	3
Columbia Generating Station	Richland	WA	4
Comanche Peak 1	Glen Rose	TX	4
Comanche Peak 2	Glen Rose	TX	4
Cooper	Nebraska City	NE	4
Crystal River 3	Crystal River	FL	2
D C Cook 1	Benton Harbor	MI	3
D C Cook 2	Benton Harbor	MI	3
Davis-Besse	Toledo	OH	3
Diablo Canyon 1	San Luis Obispo	CA	4
Diablo Canyon 2	San Luis Obispo	CA	4
Dresden 2	Morris	IL	3
Dresden 3	Morris	IL	3
Duane Arnold	Cedar Rapids	IA	3
Edwin I. Hatch 1	Baxley	GA	2
Edwin I. Hatch 2	Baxley	GA	2
Fermi 2	Toledo	MI	3

Appendix II
U.S. Commercial Nuclear Power Plants That
Are Licensed to Operate

(Continued From Previous Page)

Power plant	City	State	NRC region
Fort Calhoun	Omaha	NE	4
Ginna	Rochester	NY	1
Grand Gulf 1	Vicksburg	MS	4
H.B. Robinson 2	Florence	SC	2
Hope Creek 1	Lower Alloways Creek	NJ	1
Indian Point 2	New York	NY	1
Indian Point 3	New York	NY	1
James A. FitzPatrick	Oswego	NY	1
Joseph M. Farley 1	Dothan	AL	2
Joseph M. Farley 2	Dothan	AL	2
Kewaunee	Green Bay	WI	3
La Salle 1	Ottawa	IL	3
La Salle 2	Ottawa	IL	3
Limerick 1	Philadelphia	PA	1
Limerick 2	Philadelphia	PA	1
McGuire 1	Charlotte	NC	2
McGuire 2	Charlotte	NC	2
Millstone 2	New London	CT	1
Millstone 3	New London	CT	1
Monticello	Minneapolis	MN	3
Nine Mile Point 1	Oswego	NY	1
Nine Mile Point 2	Oswego	NY	1
North Anna 1	Richmond	VA	2
North Anna 2	Richmond	VA	2
Oconee 1	Greenville	SC	2
Oconee 2	Greenville	SC	2
Oconee 3	Greenville	SC	2
Oyster Creek	Toms River	NJ	1
Palisades	South Haven	MI	3
Palo Verde 1	Phoenix	AZ	4
Palo Verde 2	Phoenix	AZ	4
Palo Verde 3	Phoenix	AZ	4
Peach Bottom 2	Lancaster	PA	1
Peach Bottom 3	Lancaster	PA	1
Perry 1	Painesville	OH	3
Pilgrim 1	Plymouth	MA	1
Point Beach 1	Manitowoc	WI	3

Appendix II
U.S. Commercial Nuclear Power Plants That
Are Licensed to Operate

(Continued From Previous Page)

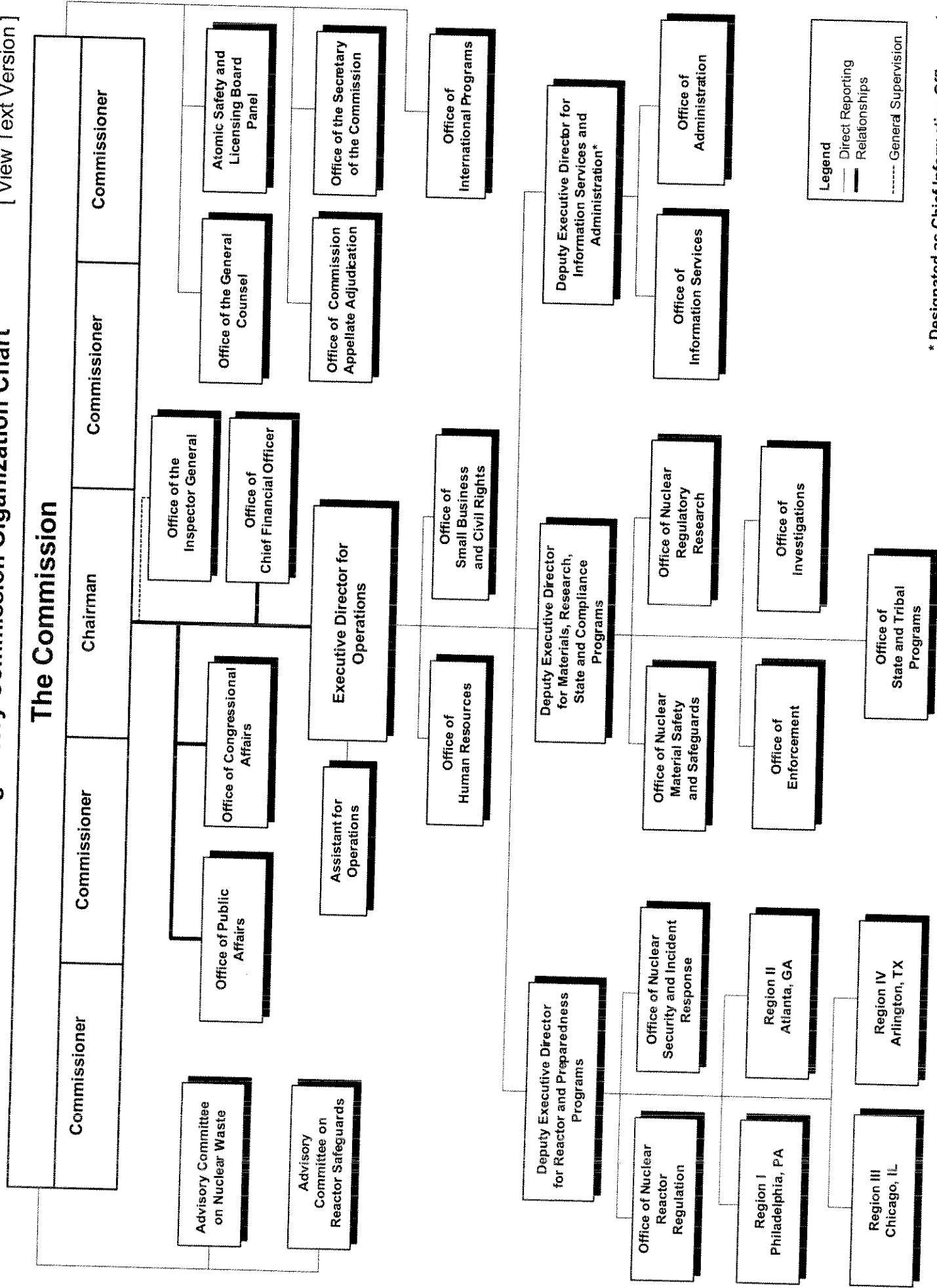
Power plant	City	State	NRC region
Point Beach 2	Manitowoc	WI	3
Prairie Island 1	Minneapolis	MN	3
Prairie Island 2	Minneapolis	MN	3
Quad Cities 1	Moline	IL	3
Quad Cities 2	Moline	IL	3
River Bend 1	Baton Rouge	LA	4
Salem 1	Lower Alloways Creek	NJ	1
Salem 2	Lower Alloways Creek	NJ	1
San Onofre 2	San Clemente	CA	4
San Onofre 3	San Clemente	CA	4
Seabrook 1	Portsmouth	NH	1
Sequoyah 1	Chattanooga	TN	2
Sequoyah 2	Chattanooga	TN	2
Shearon Harris 1	Raleigh	NC	2
South Texas Project 1	Bay City	TX	4
South Texas Project 2	Bay City	TX	4
St. Lucie 1	Ft. Pierce	FL	2
St. Lucie 2	Ft. Pierce	FL	2
Summer	Columbia	SC	2
Surry 1	Newport News	VA	2
Surry 2	Newport News	VA	2
Susquehanna 1	Berwick	PA	1
Susquehanna 2	Berwick	PA	1
Three Mile Island 1	Harrisburg	PA	1
Turkey Point 3	Miami	FL	2
Turkey Point 4	Miami	FL	2
Vermont Yankee	Battleboro	VT	1
Vogtle 1	Augusta	GA	2
Vogtle 2	Augusta	GA	2
Waterford 3	New Orleans	LA	4
Watts Bar 1	Spring City	TN	2
Wolf Creek 1	Burlington	KS	4

Source: NRC.

Attachment 2

Nuclear Regulatory Commission Organization Chart

[View Text Version]



* Designated as Chief Information Officer and Chief Freedom of Information Act Officer

Attachment 3

(2) submit to Congress a report establishing an alternative date for completion. Reports.

(d) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Secretary for research and construction activities under this subtitle (including for transfer to the Nuclear Regulatory Commission for activities under section 644 as appropriate)—

(1) \$1,250,000,000 for the period of fiscal years 2006 through 2015; and

(2) such sums as are necessary for each of fiscal years 2016 through 2021.

Subtitle D—Nuclear Security

SEC. 651. NUCLEAR FACILITY AND MATERIALS SECURITY.

42 USC 16041.

(a) SECURITY EVALUATIONS; DESIGN BASIS THREAT RULE-
MAKING.—

(1) IN GENERAL.—Chapter 14 of the Atomic Energy Act of 1954 (42 U.S.C. 2201 et seq.) (as amended by section 624(a)) is amended by adding at the end the following:

“SEC. 170D. SECURITY EVALUATIONS.

42 USC 2210d.

“a. SECURITY RESPONSE EVALUATIONS.—Not less often than once every 3 years, the Commission shall conduct security evaluations at each licensed facility that is part of a class of licensed facilities, as the Commission considers to be appropriate, to assess the ability of a private security force of a licensed facility to defend against any applicable design basis threat.

Deadline.

“b. FORCE-ON-FORCE EXERCISES.—(1) The security evaluations shall include force-on-force exercises.

“(2) The force-on-force exercises shall, to the maximum extent practicable, simulate security threats in accordance with any design basis threat applicable to a facility.

“(3) In conducting a security evaluation, the Commission shall mitigate any potential conflict of interest that could influence the results of a force-on-force exercise, as the Commission determines to be necessary and appropriate.

“c. ACTION BY LICENSEES.—The Commission shall ensure that an affected licensee corrects those material defects in performance that adversely affect the ability of a private security force at that facility to defend against any applicable design basis threat.

“d. FACILITIES UNDER HEIGHTENED THREAT LEVELS.—The Commission may suspend a security evaluation under this section if the Commission determines that the evaluation would compromise security at a nuclear facility under a heightened threat level.

“e. REPORT.—Not less often than once each year, the Commission shall submit to the Committee on Environment and Public Works of the Senate and the Committee on Energy and Commerce of the House of Representatives a report, in classified form and unclassified form, that describes the results of each security response evaluation conducted and any relevant corrective action taken by a licensee during the previous year.

“SEC. 170E. DESIGN BASIS THREAT RULEMAKING.

42 USC 2210e.

“a. RULEMAKING.—The Commission shall—

Deadlines.

"(1) not later than 90 days after the date of enactment of this section, initiate a rulemaking proceeding, including notice and opportunity for public comment, to be completed not later than 18 months after that date, to revise the design basis threats of the Commission; or

"(2) not later than 18 months after the date of enactment of this section, complete any ongoing rulemaking to revise the design basis threats.

"b. FACTORS.—When conducting its rulemaking, the Commission shall consider the following, but not be limited to—

"(1) the events of September 11, 2001;

"(2) an assessment of physical, cyber, biochemical, and other terrorist threats;

"(3) the potential for attack on facilities by multiple coordinated teams of a large number of individuals;

"(4) the potential for assistance in an attack from several persons employed at the facility;

"(5) the potential for suicide attacks;

"(6) the potential for water-based and air-based threats;

"(7) the potential use of explosive devices of considerable size and other modern weaponry;

"(8) the potential for attacks by persons with a sophisticated knowledge of facility operations;

"(9) the potential for fires, especially fires of long duration;

"(10) the potential for attacks on spent fuel shipments by multiple coordinated teams of a large number of individuals;

"(11) the adequacy of planning to protect the public health and safety at and around nuclear facilities, as appropriate, in the event of a terrorist attack against a nuclear facility; and

"(12) the potential for theft and diversion of nuclear materials from such facilities."

(2) CONFORMING AMENDMENT.—The table of sections of the Atomic Energy Act of 1954 (42 U.S.C. prec. 2011) (as amended by section 624(b)) is amended by adding at the end of the items relating to chapter 14 the following:

"Sec. 170D. Security evaluations.

"Sec. 170E. Design basis threat rulemaking."

(3) FEDERAL SECURITY COORDINATORS.—

(A) REGIONAL OFFICES.—Not later than 18 months after the date of enactment of this Act, the Nuclear Regulatory Commission (referred to in this section as the "Commission") shall assign a Federal security coordinator, under the employment of the Commission, to each region of the Commission.

(B) RESPONSIBILITIES.—The Federal security coordinator shall be responsible for—

(i) communicating with the Commission and other Federal, State, and local authorities concerning threats, including threats against such classes of facilities as the Commission determines to be appropriate;

(ii) monitoring such classes of facilities as the Commission determines to be appropriate to ensure that they maintain security consistent with the security plan in accordance with the appropriate threat level; and

Deadline.

(B) by striking "All fingerprints obtained by a licensee or applicant as required in the preceding sentence" and inserting the following:

"(2) All fingerprints obtained by an individual or entity as required in paragraph (1)";

(C) by striking "The costs of any identification and records check conducted pursuant to the preceding sentence shall be paid by the licensee or applicant." and inserting the following:

"(3) The costs of an identification or records check under paragraph (2) shall be paid by the individual or entity required to conduct the fingerprinting under paragraph (1)(A)."; and

(D) by striking "Notwithstanding any other provision of law, the Attorney General may provide all the results of the search to the Commission, and, in accordance with regulations prescribed under this section, the Commission may provide such results to licensee or applicant submitting such fingerprints." and inserting the following:

"(4) Notwithstanding any other provision of law—

"(A) the Attorney General may provide any result of an identification or records check under paragraph (2) to the Commission; and

"(B) the Commission, in accordance with regulations prescribed under this section, may provide the results to the individual or entity required to conduct the fingerprinting under paragraph (1)(A).";

(2) in subsection c.—

(A) by striking ", subject to public notice and comment, regulations—" and inserting "requirements—"; and

(B) in paragraph (2)(B), by striking "unescorted access to the facility of a licensee or applicant" and inserting "unescorted access to a utilization facility, radioactive material, or other property described in subsection a.(1)(B)";

(3) by redesignating subsection d. as subsection e.; and

(4) by inserting after subsection c. the following:

"d. The Commission may require a person or individual to conduct fingerprinting under subsection a.(1) by authorizing or requiring the use of any alternative biometric method for identification that has been approved by—

"(1) the Attorney General; and

"(2) the Commission, by regulation.".

SEC. 653. USE OF FIREARMS BY SECURITY PERSONNEL.

The Atomic Energy Act of 1954 is amended by inserting after section 161 (42 U.S.C. 2201) the following:

"SEC. 161A. USE OF FIREARMS BY SECURITY PERSONNEL.

"a. DEFINITIONS.—In this section, the terms 'handgun', 'rifle', 'shotgun', 'firearm', 'ammunition', 'machinegun', 'short-barreled shotgun', and 'short-barreled rifle' have the meanings given the terms in section 921(a) of title 18, United States Code.

"b. AUTHORIZATION.—Notwithstanding subsections (a)(4), (a)(5), (b)(2), (b)(4), and (c) of section 922 of title 18, United States Code, section 925(d)(3) of title 18, United States Code, section 5844 of the Internal Revenue Code of 1986, and any law (including regulations) of a State or a political subdivision of a State that prohibits the transfer, receipt, possession, transportation, importation, or use of a handgun, a rifle, a shotgun, a short-barreled shotgun, a short-

42 USC 2201a.

barreled rifle, a machinegun, a semiautomatic assault weapon, ammunition for any such gun or weapon, or a large capacity ammunition feeding device, in carrying out the duties of the Commission, the Commission may authorize the security personnel of any licensee or certificate holder of the Commission (including an employee of a contractor of such a licensee or certificate holder) to transfer, receive, possess, transport, import, and use 1 or more such guns, weapons, ammunition, or devices, if the Commission determines that—

“(1) the authorization is necessary to the discharge of the official duties of the security personnel; and

“(2) the security personnel—

“(A) are not otherwise prohibited from possessing or receiving a firearm under Federal or State laws relating to possession of firearms by a certain category of persons;

“(B) have successfully completed any requirement under this section for training in the use of firearms and tactical maneuvers;

“(C) are engaged in the protection of—

“(i) a facility owned or operated by a licensee or certificate holder of the Commission that is designated by the Commission; or

“(ii) radioactive material or other property owned or possessed by a licensee or certificate holder of the Commission, or that is being transported to or from a facility owned or operated by such a licensee or certificate holder, and that has been determined by the Commission to be of significance to the common defense and security or public health and safety; and

“(D) are discharging the official duties of the security personnel in transferring, receiving, possessing, transporting, or importing the weapons, ammunition, or devices.

“c. BACKGROUND CHECKS.—A person that receives, possesses, transports, imports, or uses a weapon, ammunition, or a device under subsection (b) shall be subject to a background check by the Attorney General, based on fingerprints and including a background check under section 103(b) of the Brady Handgun Violence Prevention Act (Public Law 103-159; 18 U.S.C. 922 note) to determine whether the person is prohibited from possessing or receiving a firearm under Federal or State law.

“d. EFFECTIVE DATE.—This section takes effect on the date on which guidelines are issued by the Commission, with the approval of the Attorney General, to carry out this section.”

SEC. 654. UNAUTHORIZED INTRODUCTION OF DANGEROUS WEAPONS.
Section 229 of the Atomic Energy Act of 1954 (42 U.S.C. 2278a) is amended—

(1) by striking “SEC. 229, TRESPASS UPON COMMISSION INSTALLATIONS.—” and inserting the following:

“SEC. 229. TRESPASS ON COMMISSION INSTALLATIONS.”;

(2) by adjusting the indentations of subsections a., b., and c. so as to reflect proper subsection indentations; and

(3) in subsection a.—

(A) in the first sentence, by striking “a. The” and inserting the following:

“a.(1) The”;

Attachment 4



Nuclear Power Plant Security

March 2005

Key Facts



N U C L E A R
E N E R G Y
I N S T I T U T E

SUITE 400
1776 I STREET, NW
WASHINGTON, DC

20006-3708
202.739.8000
www.nei.org

- The defense-in-depth philosophy used in the construction and operation of nuclear power plants provides high levels of protection for public health and safety.
- The Nuclear Regulatory Commission holds nuclear power plants to the highest security standards of any American industry. The industry meets or exceeds these requirements in all areas. All commercial nuclear power plants have well-armed and highly trained security forces—some 8,000 officers—that are routinely drilled and tested.
- Since Sept. 11, 2001, security has been significantly strengthened. The NRC has issued new security requirements for nuclear plant sites during the past two years, and all U.S. plants have met these requirements.
- The industry has added about 3,000 officers and upgraded physical security over the past three years. The industry has spent an additional \$1.2 billion on security since September 2001.
- Access to nuclear power plants, tightened since Sept. 11, is controlled by a physical barrier system and security officers who search all entering vehicles and people. All workers entering plant operating areas also must pass through sensitive metal and explosives detection equipment.
- Plant operators also have installed additional vehicle barrier systems to protect against vehicle bombs.
- The industry coordinates with the NRC, Department of Homeland Security and intelligence agencies on the assessment of potential threats and the specific actions by industry security forces in the event of a credible threat against a commercial nuclear facility.
- All commercial nuclear plants have emergency response procedures and contingency plans in the event of a plant accident or terrorist event. These procedures, reviewed and improved following Sept. 11, are evaluated every three years during extensive drills involving plant personnel and local police, fire and emergency management organizations. NRC and Federal Emergency Management Agency (FEMA) expert teams evaluate these drills.

Plant Security Meets All Federal Requirements

The nuclear energy industry is one of the few industries whose security program is regulated by the federal government. The NRC's requirements for nuclear power plant security are predicated on the need to protect the public from the possibility of exposure to radioactive releases caused by acts of sabotage. Intelligence information and incidents around the world are

analyzed to ensure plant protection regulations are updated to reflect potential threats.

The NRC's security regulations are designed to ensure that the industry's security force can protect against a range of threats. The threat against which the industry must defend is characterized as a suicidal, well-trained paramilitary force, armed with automatic weapons and explosives, and intent on forcing its way into a nuclear power plant to commit radiological sabotage. Such a force may have the assistance of an "insider," who could pass along information and help the attackers. The presumed goal of such an attack would be the release of radioactive material from the plant.

The NRC's "design basis threat" provides a foundation for developing defensive response strategies that cover a variety of situations. The NRC determines the design basis threat using technical studies and information received from intelligence experts and federal law enforcement agencies. It is reviewed by the agency twice a year.

Since Sept. 11, 2001, the NRC has twice raised the threat level against which nuclear plants must provide protection. In doing so, the NRC has assumed an increased number of possible attackers and weapons capabilities.

Many industry security elements are considered "safeguards" information, which means they are controlled on a "need-to-know" basis. Clearly, plant protection capabilities and response strategy should be controlled and protected from public disclosure to avoid compromises that might benefit a potential adversary.

Defense-in-Depth Against Potential Threats

The FBI considers security forces and infrastructure at nuclear power plants formidable and considers nuclear power plants difficult to penetrate.

In addition, the defense-in-depth features that protect the public from radiological hazard in the event of a reactor incident also protect the plant's fuel and related safety systems from attempted sabotage. The design of each plant emphasizes the reliability of plant systems, redundancy and diversity of key safety systems, and other safety features to prevent incidents that could pose a threat to public health and safety.

Steel-reinforced concrete containment structures protect the reactor. Redundant safety and reactor shutdown systems have been designed to withstand the impact of earthquakes, hurricanes, tornadoes and floods. Areas of the plant that house the reactor and used reactor fuel also would withstand the impact of a widebody commercial aircraft, according to peer-reviewed analyses by EPRI, a Palo Alto, Calif.-based research organization. Plant personnel are trained in emergency procedures that would be used to keep the plant safe from a sabotage attempt.

A two-day national security exercise conducted by the Center for Strategic and International Studies (CSIS) in 2002 found that nuclear power plants would be less attractive targets to terrorist organizations because of the

industry's robust security program. The exercise was designed to explore difficulties and reveal vulnerabilities that might arise if the nation were faced with a credible, but ambiguous, threat of a terrorist attack on American soil.

"Silent Vector" was developed and produced by CSIS in partnership with the ANSER Institute for Homeland Security and the Oklahoma City National Memorial Institute for the Prevention of Terrorism. Potential targets included refineries, large liquefied natural gas or liquefied petroleum gas storage operations, pipeline infrastructure, petroleum terminals, nuclear power plants, chemical operations and dams.

CSIS President John Hamre said that nuclear power plants "are probably our best-defended targets. There is more security around nuclear power plants than anything else we've got. ... One of the things that we have clearly found in this exercise is that this is an industry that has taken security pretty seriously for quite a long time, and its infrastructure, especially against these kinds of terrorist threats, is extremely good."

David McIntyre, former deputy director of the ANSER Institute for Homeland Security, added that "during the eight months of research that went into this, there were some issues like that [communication and coordination] that turned out not to be as great as we thought. And the nuclear industry was one of those that turned out to be much better connected—much more progressive, frankly—than I'd anticipated when we began the research."

Security Increased Since Sept. 11, 2001

Immediately after the events of Sept. 11, 2001, security at every nuclear power plant was placed on its highest level of alert. Nuclear plant security now is consistent with Homeland Security threat levels.

As a result, access to the plants is more strictly controlled; the defensive perimeters have been extended and reinforced, and security forces and capabilities have been augmented. Further, coordination with law enforcement, the intelligence community and the military has been enhanced. At some plants, these efforts have been supplemented by National Guard, U.S. Coast Guard, state police or other forces.

In 2002, the NRC formalized many of the enhancements to security that the industry had already implemented. The agency subsequently issued new requirements further restricting access authorization.

In April 2003, the NRC issued rules limiting the working hours of security personnel and requiring increased training including weapons proficiency. All plants met these requirements in October 2004.

Site Security Measures. All commercial nuclear plants have established extensive security measures. Plant operators and the NRC inspect these measures and test them in drills to uncover any weakness. Security measures include:

- physical barriers and illuminated detection zones
- approximately 8,000 well-trained and well-equipped armed security officers at 64 sites
- surveillance and patrols of the perimeter fence
- intrusion detection aids (including several types of detection fields, closed-circuit television systems and alarm/alert devices)
- bullet-resisting barriers to critical areas
- a dedicated contingency response force.

All threats will be countered with dedicated, tactically trained, well-armed security officers who collectively determine the nature of a threat, assess its magnitude and take aggressive steps to deter the threat.

Controlled Access. Access to a nuclear power plant requires passage through a larger “owner-controlled area” surrounding the plant.

Access to an interior fenced area—the protected area, where the reactor building is located—is controlled by security officers and physical barriers. Vehicle barriers and/or other physical boundaries ensure that the protected area of the plant cannot be breached by a direct vehicular assault or by detonation of a vehicle bomb. All vehicles, personnel and material entering the protected area first must be thoroughly inspected by security officers to ensure that no weapons, explosives or other such items are brought onto the plant site.

Access to the “protected area” of the plant is controlled through the use of physical barriers, intrusion detection equipment, closed-circuit surveillance equipment, a designated isolation zone and exterior lighting.

Access to the inner areas of the plant where vital equipment is located also is controlled through the use of physical barriers, locked and alarmed doors, and card-reader or hand geometry access control systems.

The barriers are substantial enough to effectively delay entry in order to allow for an effective armed response by plant security forces. Within the protected zone, access to all vital areas of the plant is even more secure. This access may be controlled by a security officer or provided by computer-controlled “key-card” access systems. Plant employees must have a documented need prior to gaining access to each vital area, and their movements are tracked by key-card access points throughout the vital area.

Reactor Operators Act in Concert With Security. Reactor operators train frequently to be sure they can respond to a range of unusual events. Plant operators have emergency procedures in place specifically for security situations, including automatic shutdown of the reactor in the event of an attack. Emergency planning and public notification systems support protection of public health and safety. The NRC periodically evaluates these

plans during exercises or drills, which may also involve local police, fire and emergency management organizations.

Protecting Against An Insider Threat

All nuclear power plants have programs that reduce the potential for threats from plant personnel, or “insiders.” These include authorization criteria for those allowed unescorted access to the plant’s protected area and “fitness-for-duty” programs to deter drug and alcohol abuse.

Strong behavioral observation programs are in place requiring personnel to be trained to observe and report behavior that may be a potential threat to the normal operation of a nuclear power plant. In addition, many companies provide teamwork development programs that promote commitment and accountability in the work force.

Access Authorization. Before new nuclear plant employees or contractor employees are allowed unescorted access to the protected area, they must pass several evaluations and background checks to determine whether they are trustworthy and reliable. These include drug and alcohol screening, psychological evaluations, a check with former employers, education records, criminal histories (through the FBI) and credit histories.

Fitness-for-Duty Programs. Companies that operate nuclear power plants demand and ensure that personnel perform their duties in a safe, reliable and trustworthy manner, and are not under the influence of legal or illegal substances, or mentally or physically impaired from other causes, that would adversely hinder their ability to competently perform their duties. Employees who have unescorted access to the plant’s protected area must maintain their fitness-for-duty. The NRC requires companies to conduct random drug and alcohol testing on their employees. As a result, at least half of all employees are tested annually.

Behavioral Observation. Employees with unescorted plant access are subject to continual behavioral observation programs. Behavioral observation is conducted by all personnel who have been trained to do so. The purpose is to detect individual behavioral changes, which, if left unattended, could lead to acts detrimental to public safety. Employees are offered counseling if they have job performance problems or exhibit unusual behavior. Similarly, anyone who appears to be under the influence of drugs or alcohol is immediately removed from the work area for evaluation.

Copyright © 2006 Nuclear Energy Institute.

Attachment 5

NRC ORDERS NUCLEAR POWER PLANTS TO ENHANCE SECURITY

The Nuclear Regulatory Commission has issued Orders to all 104 commercial nuclear power plants to implement interim compensatory security measures for the generalized high-level threat environment.

Some of the requirements formalize a series of security measures that NRC licensees had taken in response to advisories issued by the NRC in the aftermath of the September 11 terrorist attacks. Additional security enhancements, which have emerged from the on-going comprehensive security review, are also spelled out in the Orders. The requirements will remain in effect until such time as the Commission determines that the level of threat has diminished, or that other security changes are needed following a comprehensive re-evaluation of current safeguards and security programs. The Commission views these compensatory measures as prudent, interim measures to address the generalized high-level threat environment in a consistent manner throughout the nuclear reactor community.

The Commission recognizes that the licensees have voluntarily and responsibly implemented additional security measures following the events of September 11. But in light of the fact that the threat environment has persisted longer than expected, the Commission has concluded that it is appropriate to require certain security measures so that they are maintained within the established regulatory framework.

The specific actions taken are understandably sensitive, but generally include requirements for increased patrols, augmented security forces and capabilities, additional security posts, installation of additional physical barriers, vehicle checks at greater stand-off distances, enhanced coordination with law enforcement and military authorities, and more restrictive site access controls for all personnel.

The Orders are effective immediately.

Licensees are required to provide NRC with a schedule for achieving full compliance within 20 days. Licensees must also notify NRC within 20 days and justify in writing if they feel they are unable to comply with any of the requirements of the order, if compliance with any requirement is unnecessary in their specific circumstances, or if implementation of any requirement would cause the licensee to be in violation of the provisions of any Commission regulation or the facility license, or adversely impact safe operation of the facility.

Immediately after the September 11 attacks, the NRC advised all of the nuclear power plants and other key nuclear facilities to go to the highest level of security, which they promptly did. Specific measures were subsequently defined in a number of advisories, and have been subject to audit by NRC security experts. The NRC is coordinating with other Federal and State agencies on protection of critical infrastructure within the United States.

A copy of the non-safeguards portion of the order will be posted on the NRC web site today at: <http://www.nrc.gov> under "What's New At the Site."

Attachment 6

Fact Sheet on Nuclear Security Enhancements Since Sept. 11, 2001

Licensee Security

- The NRC took security seriously well before the September 11 terrorist attacks and has made additional enhancements since then in light of the increased threat. Enhancements of security at NRC-licensed facilities are being continually implemented notwithstanding that facilities such as nuclear power plants already had a number of security and safeguards measures in place, making them among the most robust and well protected civilian facilities in the country.
- Following the September 11 attacks, the NRC immediately advised all major licensees of nuclear facilities to go to the highest level of security. A series of Advisories, Orders and Regulatory Issue Summaries have since been issued to further strengthen security of NRC-licensed facilities and control of nuclear materials.
- The specific actions are sensitive, but generally include requirements for increased patrols, augmentation of the number and capabilities of security guards, additional security posts, installation of additional physical barriers, vehicle checks at greater stand-off distances, enhanced coordination with law enforcement and military authorities, and more restrictive site access controls for personnel.
- The NRC has underway a comprehensive review of the agency's entire safeguards and security program, regulations and procedures. The review is ongoing and has resulted in numerous security improvements.
- The NRC has studies underway to investigate potential vulnerabilities of facilities to deliberate aircraft crashes. The work in this area is ongoing. In the interim, the Commission has directed nuclear power plant licensees to develop specific plans and strategies to respond to an event that could potentially result in damage to large areas of their plants from explosions or fire. In addition, licensees must provide assurance that their emergency planning resources are sufficient to respond to such an event.
- The NRC has worked with the Federal Aviation Administration on a Notice to Airmen to prohibit planes from circling or loitering above nuclear power plants and other nuclear facilities.
- Additional measures have been put in place to provide additional protection against land attacks, including the use of a substantial vehicle bomb, and against water-borne attacks.
- The Commission is working closely with other Federal agencies to revise the design basis threat that provides the foundation for the security programs of nuclear power plant licensees. The Commission's Orders to these licensees in February 2002 effectively provide enhanced security in the interim while this work is underway.
- The NRC has expanded involvement and enhanced liaison with the Federal Bureau of Investigation, other intelligence and law enforcement agencies, NRC licensees, and military, State and local authorities.
- The NRC has established an ongoing dialogue through frequent communications with the Office of Homeland Security, the Department of Defense, the Federal Aviation Administration, the Federal Emergency Management Agency and other agencies.

- Following the 9/11 attacks, NRC-evaluated security exercises were temporarily suspended to allow licensees to focus on putting increased security measures into place. NRC has reinitiated these drills by initially exercising the table top component of the exercises that for the first time involve a wide array of Federal, State and local law enforcement and emergency planning officials. The NRC expects to expand the exercises to include a force-on-force component at the beginning of next year.
- Full security performance reviews, including force-on-force exercises, will be carried out at each nuclear power plant on a three-year cycle instead of the eight-year cycle that had been used prior to September 11, 2001.
- The NRC has developed an inter-agency response procedure involving the Department of Energy and the Federal Bureau of Investigation, among others, to cope with the threat of a radiological dispersal device. In this role, the NRC would provide technical advice to local authorities responsible for emergency response, including suggestions for protective measures, and evaluation of the radiological hazards.
- The NRC is evaluating approaches for "cradle-to-grave" control of radioactive sources which might be used in a radiological dispersal device.
- With regard to the shipment of radioactive materials and spent fuel, NRC has augmented security measures, including increased communications and additional escort and monitoring provisions.
- The NRC has increased staffing of its Headquarters Emergency Operations Center to provide a cadre of experts on call to respond to emergencies around the clock, 7 days a week. The additional staff aids in the prompt dissemination of pertinent information to all concerned, including licensees, Federal and State officials.
- The NRC established the Office of Nuclear Security and Incident Response (NSIR) in April of this year to consolidate security, safeguards and incident response responsibilities and resources and improve communication and coordination both internal and external to the agency.
- The creation of NSIR streamlines decision-making, improves the timeliness and consistency of information, and provides a more visible point of contact and effective counterpart to the Office of Homeland Security, as well as other Federal agencies.
- The NRC has developed a new Threat Advisory and Protective Measures System to communicate and respond to threats affecting NRC licensees and NRC facilities in response to Homeland Security Presidential Directive. The system corresponds to the color-coded Homeland Security Advisory System which provides a consistent national framework for allowing government officials to communicate the nature and degree of terrorist threats. The NRC system identifies specific actions to be taken by NRC licensees for each threat level to counter projected terrorist threats. The new Threat Advisory and Protective Measures System replaces the NRC's 1998 threat advisory system and covers additional classes of licensees not included in NRC's 1998 system.

Security at NRC

- On September 11, Chairman Meserve will deliver remarks to NRC staff in tribute to those who died in the attacks, as well as to their bereaved families and friends. NRC staff will observe a one-minute period of silence at 8:45 a.m. that morning, the time of the first airplane strike at the World Trade Center.

-- In addition, a host of enhanced security measures were put in place at NRC Headquarters, including the installation of concrete vehicle barriers, increased armed guards, more stringent access procedures and ongoing intra-agency communications to keep all NRC employees informed of the latest developments. Security was also bolstered at NRC regional offices.

--The NRC conducted a comprehensive review and revision of its web site to remove sensitive information which could be of interest to terrorists, while it continued to provide the public with appropriate material on the NRC and its activities.

Attachment 7



NRC NEWS

U. S. NUCLEAR REGULATORY COMMISSION

Office of Public Affairs

Washington, DC 20555-0001

Telephone 301/415-820

E-mail: opa@nrc.gov

Web Site: www.nrc.gov

No. 03-053

April 29, 2003

NRC APPROVES CHANGES TO THE DESIGN BASIS THREAT AND ISSUES ORDERS FOR NUCLEAR POWER PLANTS TO FURTHER ENHANCE SECURITY

The Nuclear Regulatory Commission, after extensive deliberation and interaction with stakeholders, has approved changes to the design basis threat (DBT). The Commission believes that the DBT represents the largest reasonable threat against which a regulated private guard force should be expected to defend under existing law. These changes will be issued by Order.

In addition, the Commission has approved the issuance of two other Orders to nuclear plants regarding work hours, training, and qualification requirements for security personnel to further enhance protection of public health and safety, as well as the common defense and security. The three Orders will be issued to all 103 operating commercial nuclear power plants.

The three Orders, which are being issued today, will be effective immediately, but allow transition periods for full implementation. With these actions, the Commission expects that there will be a period of regulatory stability during which operating commercial plant licensees will be able to consolidate these and previously ordered security enhancements.

These Orders, in combination with the recently-issued Order in the area of access authorization, enhance the already strong defense capability at these sites using three interdependent elements directed to best protect the public, with the appropriate resources placed at the right places. These elements are:

- the revised Design Basis Threat and associated defensive capabilities derived from previous measures that the Commission directed;
- tighter work hour control and more robust training requirements for security personnel, to increase their capability to respond to threats; and
- enhanced access authorization controls to ensure all plant personnel with access to critical areas have had the most rigorous background checks permitted by law.

The Order that imposes revisions to the Design Basis Threat requires power plants to implement additional protective actions to protect against sabotage by terrorists and other adversaries. The details of the design basis threat are safeguards information pursuant to Section 147 of the Atomic Energy Act and will not be released to the public. This Order builds on the changes made by the Commission's February 25, 2002 Order. The Commission believes that this DBT represents the largest reasonable threat against which a regulated private security force should be expected to defend under existing law. It was arrived at after extensive deliberation and interaction with cleared stakeholders from other Federal agencies, State governments and industry.

Under NRC regulations, power reactor licensees must ensure that the physical protection plan for each site is designed and implemented to provide high assurance in defending against the DBT to ensure adequate protection of public health and safety and common defense and security. Extensive changes in those physical protection plans will now be made and submitted to NRC for approval.

The second Order describes additional measures related to security force personnel fitness for duty and security force work hours. It is to ensure that excessive work hours do not challenge the ability of nuclear power plant security forces to remain vigilant and effectively perform their duties in protecting the plants. However, the Order does include provisions to allow increases in work hours under certain conditions, once specific requirements are met. The NRC developed this unclassified Order through a public process. The NRC carefully considered comments from power reactor licensees, security force personnel, public citizen groups and other agencies in reaching its final decision. The Order will be publicly available on NRC's website at: <http://www.nrc.gov>.

The third Order describes additional requirements related to the development and application of an enhanced training and qualification program for armed security personnel at power reactor facilities. These additional measures include security drills and exercises appropriate for the protective strategies and capabilities required to protect the nuclear power plants against sabotage by an assaulting force. This Order requires more frequent firearms training and qualification under a broader range of conditions consistent with site-specific protective strategies. The details of the enhanced training requirements are safeguards information, and will not be released to the public. As with the DBT Order, the Commission solicited comments on a draft training Order from cleared stakeholders, including security personnel and took those comments under consideration in reaching its final decision.

"With the completion of these complementary Orders," Chairman Nils J. Diaz said, "the public should be reassured that the nation's nuclear power plants are well-secured against potential threats. The NRC intends to continue working closely with the Department of Homeland Security and other Federal agencies, as well as with State and local law enforcement and emergency planning officials to ensure an overall integrated approach to the security of these critical facilities."

###

Attachment 8

CRS Report for Congress

Received through the CRS Web

Nuclear Power Plants: Vulnerability to Terrorist Attack

Carl Behrens and Mark Holt
Specialists in Energy Policy
Resources, Science, and Industry Division

Summary

Protection of nuclear power plants from land-based assaults, deliberate aircraft crashes, and other terrorist acts has been a heightened national priority since the attacks of September 11, 2001. The Nuclear Regulatory Commission (NRC) has strengthened its regulations on nuclear reactor security, but critics contend that implementation by the industry has been too slow and that further measures are needed. Several provisions to increase nuclear reactor security are included in the Energy Policy Act of 2005, signed August 8, 2005. The new law requires NRC to conduct “force on force” security exercises at nuclear power plants at least once every three years and to revise the “design-basis threat” that nuclear plant security forces must be able to meet, among other measures. This report will be updated as events warrant.

Nuclear power plants have long been recognized as potential targets of terrorist attacks, and critics have long questioned the adequacy of the measures required of nuclear plant operators to defend against such attacks. Following the September 11, 2001, attacks on the Pentagon and the World Trade Center, the Nuclear Regulatory Commission (NRC) began a “top-to-bottom” review of its security requirements. On February 25, 2002, the agency issued “interim compensatory security measures” to deal with the “generalized high-level threat environment” that continued to exist, and on January 7, 2003, it issued regulatory orders that tightened nuclear plant access. On April 29, 2003, NRC issued three orders to restrict security officer work hours, establish new security force training and qualification requirements, and increase the “design basis threat” that nuclear security forces must be able to defeat.

Security Regulations

Under the regulations in place prior to the September 11 attacks, all commercial nuclear power plants licensed by NRC must be protected by a series of physical barriers and a trained security force. The plant sites are divided into three zones: an “owner-controlled” buffer region, a “protected area,” and a “vital area.” Access to the protected area is restricted to a portion of plant employees and monitored visitors, with stringent

access barriers. The vital area is further restricted, with additional barriers and access requirements. The security force must comply with NRC requirements on pre-hiring investigations and training.¹

Design Basis Threat. The severity of attacks to be prepared for are specified in the form of a “design basis threat” (DBT). One of NRC’s April 2003 regulatory orders changed the DBT to “represent the largest reasonable threat against which a regulated private guard force should be expected to defend under existing law,” according to the NRC announcement. The details of the revised DBT, which took effect October 29, 2004, were not released to the public.

NRC requires each nuclear power plant to conduct periodic security exercises to test its ability to defend against the design basis threat. In these “force on force” exercises, monitored by NRC, an adversary force from outside the plant attempts to penetrate the plant’s vital area and damage or destroy key safety components. Participants in the tightly controlled exercises carry weapons modified to fire only blanks and laser bursts to simulate bullets, and they wear laser sensors to indicate hits. Other weapons and explosives, as well as destruction or breaching of physical security barriers, may also be simulated. While one squad of the plant’s guard force is participating in a force-on-force exercise, another squad is also on duty to maintain normal plant security. Plant defenders know that a mock attack will take place sometime during a specific period of several hours, but they do not know what the attack scenario will be. Multiple attack scenarios are conducted over several days of exercises.

Full implementation of the force-on-force program coincided with the effective date of the new DBT in late 2004. Standard procedures and other requirements have been developed for using the force-on-force exercises to evaluate plant security and as a basis for taking regulatory enforcement action. Many tradeoffs are necessary to make the exercises as realistic and consistent as possible without endangering participants or regular plant operations and security. Each plant is required to conduct NRC-monitored force-on-force exercises once every three years.

NRC required the nuclear industry to develop and train a “composite adversary force” comprising security officers from many plants to simulate terrorist attacks in the force-on-force exercises. However, in September 2004 testimony, the Government Accountability Office (GAO) criticized the industry’s selection of a security company that guards about half of U.S. nuclear plants, Wackenhut, to also provide the adversary force. In addition to raising “questions about the force’s independence,” GAO noted that Wackenhut had been accused of cheating on previous force-on-force exercises by the Department of Energy.²

¹ General NRC requirements for nuclear power plant security can be found at 10 CFR 73.55.

² Government Accountability Office. *Nuclear Regulatory Commission: Preliminary Observations on Efforts to Improve Security at Nuclear Power Plants*. Statement of Jim Wells, Director, Natural Resources and Environment, Government Accountability Office, to the Subcommittee on National Security, Emerging Threats, and International Relations, House Committee on Government Reform. September 14, 2004. p. 14.

Congress imposed statutory requirements for the DBT and force-on-force exercises in the Energy Policy Act of 2005, signed August 8, 2005. The act requires that each nuclear plant undergo force-on-force exercises at least once every three years (NRC's current policy), that the exercises simulate the threats in the DBT, and that NRC "mitigate any potential conflict of interest that could influence the results of a force-on-force exercise, as the Commission determines to be necessary and appropriate."

The new law requires NRC to revise the DBT within 18 months, after considering a wide variety of potential modes of attack (physical, chemical, biological, etc.), the potential for large attacks by multiple teams, potential assistance by several employees inside a facility, the effects of large explosives and other modern weaponry, and other specific factors.

Emergency Response. After the 1979 accident at the Three Mile Island nuclear plant near Harrisburg, PA, Congress required that all nuclear power plants be covered by emergency plans. NRC requires that within an approximately 10-mile Emergency Planning Zone (EPZ) around each plant the operator must maintain warning sirens and regularly conduct evacuation exercises monitored by NRC and the Federal Emergency Management Agency (FEMA). In light of the increased possibility of terrorist attacks that, if successful, could result in release of radioactive material, critics have renewed calls for expanding the EPZ to include larger population centers.

Another controversial issue regarding emergency response to a radioactive release from a nuclear power plant is the distribution of iodine pills. A significant component of an accidental or terrorist release from a nuclear reactor would be a radioactive form of iodine, which tends to concentrate in the thyroid gland of persons exposed to it. Taking a pill containing non-radioactive iodine before exposure would prevent absorption of the radioactive iodine. Emergency plans in many states include distribution of iodine pills to the population within the EPZ, which would protect from exposure to radioactive iodine, although giving no protection against other radioactive elements in the release. NRC in 2002 began providing iodine pills to states requesting them for populations within the 10-mile EPZ.

Nuclear Plant Vulnerability

Operating nuclear reactors contain large amounts of radioactive fission products which, if dispersed, could pose a direct radiation hazard, contaminate soil and vegetation, and be ingested by humans and animals. Human exposure at high enough levels can cause both short-term illness and death, and longer-term deaths by cancer and other diseases.

To prevent dispersal of radioactive material, nuclear fuel and its fission products are encased in metal cladding within a steel reactor vessel, which is inside a concrete "containment" structure. Heat from the radioactive decay of fission products could melt the fuel-rod cladding even if the reactor were shut down. A major concern in operating a nuclear power plant, in addition to controlling the nuclear reaction, is assuring that the core does not lose its coolant and "melt down" from the heat produced by the radioactive fission products within the fuel rods. Therefore, even if plant operators shut down the reactor as they are supposed to during a terrorist attack, the threat of a radioactive release would not be eliminated.

Commercial reactor containment structures — made of steel-reinforced concrete several feet thick — are designed to prevent dispersal of most of a reactor's radioactive material in the event of a loss of coolant and meltdown. Without a breach in the containment, and without some source of dispersal energy such as a chemical explosion or fire, the radioactive fission products that escaped from the melting fuel cladding mostly would remain where they were. The two major meltdown accidents that have taken place in power reactors, at Three Mile Island in 1979 and at Chernobyl in the Soviet Union in 1986, illustrate this phenomenon. Both resulted from a combination of operator error and design flaws. At Three Mile Island, loss of coolant caused the fuel to melt, but there was no fire or explosion, and the containment prevented the escape of substantial amounts of radioactivity. At Chernobyl, which had no containment, a hydrogen explosion and a fierce graphite fire caused a significant part of the radioactive core to be blown into the atmosphere, where it contaminated large areas of the surrounding countryside and was detected in smaller amounts literally around the world.

Vulnerability from Air Attack. Nuclear power plants were designed to withstand hurricanes, earthquakes, and other extreme events, but attacks by large airliners loaded with fuel, such as those that crashed into the World Trade Center and Pentagon, were not contemplated when design requirements were determined. A taped interview shown September 10, 2002, on Arab TV station al-Jazeera, which contains a statement that Al Qaeda initially planned to include a nuclear plant in its 2001 attack sites, intensified concern about aircraft crashes.

In light of the possibility that an air attack might penetrate the containment building of a nuclear plant, some interest groups have suggested that such an event could be followed by a meltdown and widespread radiation exposure. Nuclear industry spokespersons have countered by pointing out that relatively small, low-lying nuclear power plants are difficult targets for attack, and have argued that penetration of the containment is unlikely, and that even if such penetration occurred it probably would not reach the reactor vessel. They suggest that a sustained fire, such as that which melted the structures in the World Trade Center buildings, would be impossible unless an attacking plane penetrated the containment completely, including its fuel-bearing wings.

Recently completed NRC studies “confirm that the likelihood of both damaging the reactor core and releasing radioactivity that could affect public health and safety is low,” according to NRC Chairman Nils Diaz. However, NRC is considering studies of additional measures to mitigate the effects of an aircraft crash.³

Spent Fuel Storage. Radioactive “spent” nuclear fuel — which is removed from the reactor core after it can no longer efficiently sustain a nuclear chain reaction — is stored in pools of water in the reactor building or in dry casks elsewhere on the plant grounds. Because both types of storage are located outside the reactor containment structure, particular concern has been raised about the vulnerability of spent fuel to attack by aircraft or other means. Spent fuel pools and dry cask storage facilities are subject to NRC security requirements.

³ Letter from NRC Chairman Nils J. Diaz to Secretary of Homeland Security Tom Ridge, September 8, 2004.

The primary concern is whether terrorists could breach the thick concrete walls of a spent fuel pool and drain the cooling water, which could cause the spent fuel's zirconium cladding to overheat and catch fire. A report released in April 2005 by the National Academy of Sciences (NAS) found that "successful terrorist attacks on spent fuel pools, though difficult, are possible," and that "if an attack leads to a propagating zirconium cladding fire, it could result in the release of large amounts of radioactive material." NAS recommended that the hottest spent fuel be interspersed with cooler spent fuel to reduce the likelihood of fire, and that water-spray systems be installed to cool spent fuel if pool water were lost. The report also called for NRC to conduct more analysis of the issue and consider earlier movement of spent fuel from pools into dry storage.⁴

Both the House- and Senate-passed versions of the FY2006 Energy and Water Development appropriations bill (H.R. 2419, H.Rept. 109-86, S.Rept. 109-84) would provide \$21 million for NRC to carry out the NAS recommendations. The House Appropriations Committee was particularly critical of NRC's actions on spent fuel storage security: "The Committee expects the NRC to redouble its efforts to address the NAS-identified deficiencies, and to direct, not request, industry to take prompt corrective actions."

Regulatory and Legislative Proposals

Critics of NRC's security measures have demanded both short-term regulatory changes and legislative reforms.

A fundamental concern was the nature of the DBT, which critics contended should be increased to include a number of separate, coordinated attacks. Critics also contended that nearly half of the plants tested in NRC-monitored mock attacks before 9/11 failed to repel even the small forces specified in the original DBT, a charge that industry sources vigorously denied. Critics also pointed out that licensees are required to employ only a minimum of five security personnel on duty per plant, which they argue is not enough for the job.⁵ Nuclear spokespersons responded that the actual security force for the nation's 65 nuclear plant sites numbers more than 5,000, an average of about 75 per site (covering multiple shifts). Nuclear plant security forces are also supposed to be aided by local law enforcement officers if an attack occurs.

In February 2002, NRC implemented what it called "interim compensatory security measures," including requirements for increased patrols, augmented security forces and capabilities, additional security posts, installation of additional physical barriers, vehicle checks at greater stand-off distances, enhanced coordination with law enforcement and military authorities, and more restrictive site access controls for all personnel. The further

⁴ National Academy of Sciences, Board on Radioactive Waste Management, *Safety and Security of Commercial Spent Nuclear Fuel Storage, Public Report* (online version), released April 6, 2005.

⁵ 10 CFR 73.55 (h)(3) states: "The total number of guards, and armed, trained personnel immediately available at the facility to fulfill these response requirements shall nominally be ten (10), unless specifically required otherwise on a case by case basis by the Commission; however, this number may not be reduced to less than five (5) guards."

orders issued April 29, 2003, expanded on the earlier measures, including revising the DBT, which critics continue to describe as inadequate. Continuing congressional concerns resulted in the new criteria in the Energy Policy Act of 2005 for further DBT revisions.

Because of the growing emphasis on security, NRC established the Office of Nuclear Security and Incident Response on April 7, 2002. The office centralizes security oversight of all NRC-regulated facilities, coordinates with law enforcement and intelligence agencies, and handles emergency planning activities. Force-on-force exercises are an example of the office's responsibilities. On June 17, 2003, NRC established the position of Deputy Executive Director for Homeland Protection and Preparedness, whose purview includes the Office of Nuclear Security and Incident Response.

Legislation. Since the 9/11 attacks, numerous legislative proposals, including some by NRC, have focused on nuclear power plant security issues. Several of those ideas, such as the revision of the design-basis threat and the force-on-force security exercises, were included in the Energy Policy Act of 2005, which also includes:

- assignment of a federal security coordinator for each NRC region;
- backup power for nuclear plant emergency warning systems;
- tracking of radiation sources;
- fingerprinting and background checks for nuclear facility workers;
- authorizing use of firearms by nuclear facility security personnel (preempting some state restrictions);
- authorizing NRC to regulate dangerous weapons at licensed facilities;
- extending penalties for sabotage to cover nuclear facilities under construction;
- requiring a manifest and personnel background checks for import and export of nuclear materials; and
- requiring NRC to consult with the Department of Homeland Security on the vulnerability to terrorist attack of locations of proposed nuclear facilities before issuing a license.

A number of legislative proposals introduced since 9/11 to increase nuclear plant security were not included in the new law, including the creation of a federal force within the NRC to replace the private guards at nuclear power plants, requiring emergency planning exercises within a 50-mile radius around each nuclear plant, and stockpiling iodine pills for populations within 200 miles of nuclear plants. Other measures proposed but not enacted include a task force to review security at U.S. nuclear power plants and a federal team to coordinate protection of air, water, and ground access to nuclear power plants.